NEBULA AI（NBAI）
分散型AIブロックチェーン
ホワイトペーパー

Nebula AI Team

2018 年2 月

注意書き

本文は Nebula AI プラットフォーム及び生態システムを紹介するテクノロジーホワイトペーパーであり、未来の計画とみなすことができません。その他の記述がない限り、本文で述べた製品は現在開発中であり、Nebula AI は技術及びプロジェクトの成功を保障しません。法律許容の範囲で、法律およびほかの方式の暗示と保障を提供しません。Nebula AI の技術、Nebula AI とのインタラクションなどについて、本文の内容に基づき何等かの結論及び決定を行うことはできません。本文で述べた Nebula AI プラットフォーム及び生態システムについての情報、問い合わせなどによる損害が生じる場合（予知できるかどうか関係なく）、ミスや不注意があっても Nebula AI は一切責任を負いません。

本文の情報は信頼可能だとされる情報源から由来したが、Nebula AI は該当情報の完全性、適用性、精確性を担保しません。すべての関係者は上記の情報に基づき決定を行うことができません。本文の情報は作者現在の考えであり、Nebula AI と一致しない場合もあり、また、情報が変更される可能性も存在し、もう一度知らせません。本文が述べた内容が変更される場合、Nebula AI はこのファイルを修正し、あるいは他の方式で読者に通知する義務を持っていません。

本文の内容あるいはミスによる損害が生じる場合、Nebula AI 及びその関係者が一切責任を負いません。本文で述べた予測、前景、意思表示などに対し、Nebula AI 及びその顧問たちは実際を確認していません。我々は情報の正確さを保つよう最大限の努力をしたが、本文で述べた予測、判断などはこの段階の合理的な仮説であり、将来事項に対する宣言だとみなすことができません。本文で言及したすべての計画、予測、予報、前景、意思表示は技術の進展、法律、政策、市場変動、企業行為などにより、実現できないリスクが存在しています。読者は自分の知識、調査、評価などで判断すべきです。

本文は www.nebula-ai.com のみからアクセスできます。Nebula AI による書面の承諾を得なければ、本文を再配布することは断固禁じられます。本文へアクセスすれば上述の制限を同意したとみなされます。

要旨

ブロックチェーンは人々にデジタル化のトラストメカニズムを提供し、価値伝達の効率を上げ、コストを下げました。高効率かつ信用可能な価値のインターネットが到来しました。同時に、ブロックチェーンアプリケーションのイノベーションも活気にあふれており、公共サービスの発展と業界の未来を示しています。近年、人工知能は著しく発展しており、グローバル範囲で研究と応用のブームが来ました。人工知能はすでに社会の様々な面に浸透し、これからも人類社会の変革を促進し続けます。

Nebula AI は分散型の人工知能コンピューティング基礎チェーン（NBAI）を作ることを目的にしています。これにより、GPU マイニングマシンを人工知能コンピューティング用のマシンに転化し、POW によるエネルギーの浪費を削減します。Nebula AI ブロックチェーンでは、開発者は Nebula AI が提供した API を利用し人工知能 APP を開発することが可能です。無料あるいは有料の APP、ユーザーの支払などから NBAI トークンを得ることができます。NBAI に記録された取引は改ざん防止です。また、分散型のコンピューティングも高度の並行性とローレイテンシーを保障しています。GPU マイニングマシンの転用はより経済的、効率よい人工知能サービスを可能にしました。

Nebula AI はすでにカナダにおいて AI 人材育成センターを作り、AI 領域の最新技術の発信と人材の育成を行っています。このほか、一つの 10MW の人工知能コンピューティングセンターがデザインされています。システムが搭載する画像同定、数理ファイナンスなどのアプリケーションも同時に開発されています。

完成した NBAI 生態システムは DAI App、科学研究アプリケーション、大学教育などの上層アプリケーションと NBAI ブロックチェーン、AI マイニングマシン、人工知能データセンターなどの基礎サポートを整合します。革新的な NBAI 生態システムの経済モデルは価値伝達、経済価値上昇のシステムを実現します。

目次

1　技術と業界概況

1.1　価値のインターネットの現状

従来のインターネットは歴史的内容に基づくものであり、新しい価値を作ることができなく、業界では情報のインターネットといわれます。ブロックチェーン技術は効率的且つ信頼可能な価値伝達システムを作ることで、従来のインターネットを社会のトラスト体系を構築するネットワークに進化させ、新しい価値を生み出し、有効な価値伝達を可能にしました。それゆえ、業界では価値のインターネットといわれます

1.1.1　ブロックチェーンの発展

ブロックチェーン技術は分散型システム、インターネット、暗号学、データ構造など複数領域の研究成果に基づき発展してきた総合技術システムです。ブロックチェーンでは、多くの参入者が共同でデータの記録と維持を行い、暗号学を通じデータの伝達とアクセスの安全を保ちます。データはチェーンに貯蔵され、改ざん防止という特性を持っています。ビットコイン・イーサリアムを代表とするブロックチェーン技術は暗号化、コンセンサスメカニズム、タイムスタンプ、経済報酬などの手段で分散型のノードの間で P2P 信用取引を実現しました。従来の中心型の機構では、取引は効率が低く、コストが高く、データの安全も確保されません。ブロックチェーン技術を通じこれらの問題を解決できると考えられます。ブロックチェーン技術を通じ、参入者たちは情報を共有し、共同でプロジェクトを運営することができます。そのため、このようなシステムは大多数の信頼関係に基づくビジネスモデルと組織構成に応用できます。

Satoshi Nakamoto は 2008 年に、ビットコインをデザインする論文 A Peer-to-Peer Electronic Cash System を発表しました。作者は新らな分散型デジタル支払システムを作ることを望んでいます。このシステムは信頼関係ではなく暗号学原理に基づくものであり、第三者の中心型機構がなくても取引することができます[13]。この論文が発表してから、ビットコインを代表とするブロックチェ

ーン技術が人々に知られるようになりました。

業界と学界では、ブロックチェーン技術は二世代に分けられます。

- 1.0 ビットコイン —暗号化台帳と分散型支払という問題を解決しました。
- 2.0 イーサリアム —スマートコントラクトを導入することで、仮想機械とコントラクトプログラミングが可能になり、暗号通貨の発展に新な示唆を与え、ブロックチェーン技術の応用価値を豊富にしました。これにより、多くのDAppが誕生し、ICO金融も盛んになり、金融市場に新たな分野が出現しました。

ビットコインはブロックチェーン最初のアプリケーションとして、分散型の暗号通貨システムを実現しました。ビットコインは特定のアルゴリズムに基づき、一定のコンピューティングタスクを完成することで生成され、個人や機構に頼ることはありません。これによりビットコイン分散型台帳システムの一致性が保たれます。Vitalik Buterin はイーサリアムにて、スマートコントラクトという概念を導入し、チューリング完全のブロックチェーン通用フレームワークを提供しました[4]。ブロックチェーン技術を応用することで P2P 情報伝送システムを作ること、新たな信頼メカニズムを作ることができます。共同管理と公開的取引を実現すると同時に、個人の権益とノードのプライバシーが保護されます。このメカニズムは価値伝達の効率を上げ、コストを下げ、デジタル経済を新たな段階へ導き、効率よくかつ信頼可能な価値のインターネットを作ってくれます。同時に、ブロックチェーンアプリケーションが盛んになり、公共サービスと産業イノベーションの発展が促進されます。

1.1.2 DAPP と人工知能

DApp（Decentralized Application）はコードが分散型 P2P ネットワークサーバノードにおいて実行されているアプリケーションであり、フロントエンドプレゼンテーション層、バックグラウンドサーバ、スマートコントラクトという三つの部分に構成されます。イーサリアムの迅速の発展により、各業界において数十万の DAPP がすでに誕生し、価値のインターネットは日々進化し続けています。

近年、人工知能領域では突破が多くみられ、グローバルにおいて研究のブームをもたらしています。人工知能の研究とアプリケーションはすでに社会の隅々までに入り込み、人工知能に関する DApp も多くみられます。しかし、人

工知能の研究は大規模の計算力が必要であり、すでに初期の CPU 計算から GPU 計算に代わり、大規模のデプロイを実現させるには、ハードウェア性能と並行処理性能が問われます。

Nebula AI ブロックチェーンは次世代の人工知能ブロックチェーンとして、AI 時代における計算能力の需要を満たすこと、リソースの地域間の流通を実現させること、人工知能 DAPP の開発を容易にすることを目的にしています。これにより、ブロックチェーンの少額決済、ハイパーレッジャー、分散型などの特性と人工知能アプリケーションを完璧に結合させ、DApp + AI から DAI App へという目標を実現します。

Nebula AI は分散型人工知能コンピューティング基礎チェーンです。GPU マイニングマシンを AI コンピューティングに使用することで従来の POW によるエネルギーの浪費を削減します。Nebula AI ブロックチェーンにおいて、開発者は Nebula AI の SDK、API を利用し人工知能 APP を開発でき、無料あるいは有料の APP、ユーザーの支払などから NBAI トークンを得ることができます。ユーザーの支払の一部分は人工知能 APP の収入になり、一部分は人工知能 APP を通じ Nebula AI ブロックチェーンに支払われます。NBAI に記録された取引は改ざん防止で、分散型コンピューティングネットワークにより十分なコンピューティング能力も保障され、GPU マイニングマシンの転用も低価格の人工知能サービスを可能にしました。Nebula AI はすでにカナダにおいて AI 人材育成センターを作り、AI 領域の最新技術の発信と人材の育成を行っています。このほか、一つの 10MW の人工知能コンピューティングセンターがデザインされています。システムが搭載する画像同定、数理ファイナンスなどのアプリケーションも同時に開発されています。これから Nebula AI は価値のインターネットの発展を促進し、世界の人工知能開発に効率的且つ低価格の基礎サービスを提供します。

1.2 市場前景

ブロックチェーンはすでに多くの業界に応用されています。各国はブロックチェーンの進展に注目しており、実際の応用を図っています。市場調査機構 Gartner によると、ブロックチェーンに基づく業務は 2020 年までに 1000 億ドルに上るということです。金融界のほか、製造業、サプライチェーン業界においても一万憶ドル以上の価値を生み出すと考えられます。Klaus Schwab によれ

ば、ブロックチェーンは機械化、電力化、デジタル化に次いでの第四回の工業革命であり、2025 年までに、世界の GDP の 10%がブロックチェーンにより貯蔵される見込みです[18]。Marketsand　Markets の予測では、企業効率を上げるブロックチェーン解決案を提供する企業の年平均成長率は 2016 年から 2021 にかけてピークに達します[9]。ブロックチェーン技術は主に社会公共サービスと経済モデルの最適化に応用されます。

社会公共サービスについて、ブロックチェーン技術は社会保障、著作権、公共管理などに浸透しており、主に身分認識、権益認証、情報共有、政務公開という四つの領域をめぐって発展しています。イギリス政府は 2016 年に『ブロックチェーン:分散型台帳技術』という報告を出しており、初めて国家レベルでブロックチェーンを政府業務に応用する可能性を探索した[21]。その後、アメリカが「国会ブロックチェーングループ」を成立し、ロシア、シンガポール、ドバイ、日本、中国みなブロックチェーンの社会応用に力を入れています[15]。ブロックチェーン技術の分散式コンセンサス、オープンソース、社会協力などの哲学を応用することで、公共サービスにおいてのデータ管理を最適化し、管理原則を変化させ、民衆の参入度を上げ、運営のコストを下げ、管理の質と効率を向上させることなどができます。

経済モデルの最適化について、ブロックチェーンはただの技術革命ではなく、ビジネスモデルを再築し次世代の金融と経済を作ることを目的としています。2015 年にも、ブロックチェーン業界はすでにアメリカベンチャーキャピタルで最高額の融資を獲得しました。現在、世界ではブロックチェーンプロジェクトはすでに 2000 個を超え、暗号学資産の総額は 900 億ドルに達しています。ブロックチェーンは金融、共有経済、モノのインターネットなどに応用することが期待されており、ゴールドマン、シティグループ、ナスダック、デロイト、エアビーアンドビーなどがすでにこの業界に参入しており、暗号学資産に投資する人数も著しく増加しており、2013 年初の 200 万から 2017 年初の 2000 万に増えました[19]。ブロックチェーン体系では、参入者は相手の情報が知らなくても取引することができ、「信頼関係に頼らないトラスト」を実現し、従来の中心機構に基づく信頼関係を変化させ、取引の双方は直接価値を交換できます。このようなブロックチェーン経済に基づく解決案は現在のビジネスルールを変え、新な協力モードを作ることができます。ブロックチェーンは社会経済のグレードアップを体系的に支えます。このような優位性はすでに金融サービス、サプライチェーン管理、スマート製造、教育、雇用などの各業界で見られ

ます。

人工知能産業は 60 年間の浮き沈みを経て、機械学習の発展につれ回復し、現在では世界において重要な位置を占め、多くの国は人工知能の探索に力を入れています。人工知能の市場規模は 2015 年に 1683.9 億に達し、2016 年において、各領域から注目を集め、総額は 1900 億を超えました[12]。市場のニーズに合わせ、予測では、市場規模は 2018 年に 2700 億になる見込みです。

将来では、DAPP は価値のインターネットの主幹となると考えられます。人工知能もすべての応用領域と関わる見込みです。ブロックチェーンは両者を支える基礎施設として大いに発展し、従来のインターネット、人間社会、自然環境を大きく変革させると考えられます。

1.3 現存する問題

1. 高度の中心化

グーグル、アマゾンなどは人工知能のコンピューティングサービスを提供しているが、ビジネス会社であるため、自身の利益あるいは政府の圧力により、サービスを中止する可能性が存在しています。例として、グーグルは中国において政府の規制によりサービスを提供することができません。

ブロックチェーンは新たな分散型プロトコルであり、分散型台帳（多くのアドレス、地域に分布するデータベース）に基づき、安全にデータを貯蔵しています[3]。分散型の構造に基づくため、ノードの権益と義務は平等です。また、グローバルに分布するノードにより認証を行い、データの安全が確保されます。技術により取引を行い、第三者の中心化機構に頼る必要はありません。企業は分散型台帳技術を用いて取引を処理し、台帳に貯蔵します。多くの参入者がコンセンサスに達すれば、すべての記録がタイムスタンプによる署名を獲得できます。分散型台帳のすべての参入者は記録を回覧し検証することができます[11]。そのため、稼働中のノードが一つさえあればネットワーク全体を停止することができません。この技術を通じ、閉鎖不可能な分散型 AI クラウドサービスを作ることが可能です。

2. データプライバシー安全

中心型の会社において各種のプロトコルが存在するが、内部の職員が情報を漏らすことがあります。また、政府からデータを要求される場合も存在し、ユーザーのデータの安全は十分保護されません。ブロックチェーンは暗号学技術

に基づき、特定のアルゴリズムと一定のコンセンサスメカニズムを通じデータを各ノードに貯蔵し、中心化機構に頼る必要はありません。暗号学技術に基づくトラスト関係はコストが低く、安全性が高く、カスタマイズもできます[22]。すべてのノードは完全なデータを記録することでデータの安全性と精確さが守られます。P2P 暗号化技術を通じ、私有鍵暗号の所有者以外の人はデータへアクセスができても解読し使用することができません。これは高価値のデータとモデルトレニンーグに重要な意義を持っています。データ安全について、ブロックチェーンの長所は以下のとおりです。

- 冗長性のデータベースを利用しデータの完全さを保護
- 暗号学の原理を利用しデータを検証し、改ざん防止という特性を確保
- マルチ私有鍵暗号でアクセス権限をコントロール

3. 維持のコスト

中心型のコンピューティングセンターでは人件費が高いです。それに対し、ブロックチェーンの少額決済の機能を利用すれば、維持費用の支払が簡単になり、だれでもコンピューティング能力を他人に貸すことができます。このような共有経済は人件費を著しく削減することで、コンピューティングのコストを下げます。

4. ハッシュ計算能率

現在では、イーサリアム、Zcash などの POW は大量の電力を消費しています。単純な POW より、このよう計算能力を AI コンピューティングに応用したほうが遥かに有意義です。最新の研究によれば、毎年ビットコインマイニングが消耗した電気は 159 か国の平均電気消費量を超えています[1]。このような高額な電気消費問題は解決されなければなりません。Digiconomist によればビットコインマイニングは一年間で 約 30.14TWh の電気を消費し、アイルランドの 25 TWh をはるかに上回っています。また、オランダ銀行の論文では、一回のビットコイン取引が消耗した電気は一世代の一か月の消費量に等しいと指摘されています。そのほか、Digiconomist は暗号通貨二位のイーサリアムが消耗した電気も多くの国を超えているということを述べました[1]。

5. ブロックチェーン生態システムの建立

ブロックチェーンのアプリケーション（DAPP）の増加につれ、良好な生態システムがますます重要になってきた。例えばユーザーが DAPP をどうやって検索できるのか、どうやって開発者を補助するのかなどがあげられます。例としてイーサリアムでは、DAPP の数は 10 万個以上を超えており、如何にそ

の中で必要とする DAPP を見出すのかは極めて重要です。ブロックチェーン技術の普及につれ、暗号通貨のほか、多くの応用場面が見えてきました。例えば、イーサリアムを代表とするコミュニティはスマートコントラクトという概念を導入し、Ripple はブロックチェーン技術により即時グロス決済を実現しました。応用場面の多様化により、ユーザーのニーズも増加し多くの課題が残っています。

1.4 プロジェクトの目標

現在の中心型のクラウドコンピューティングの状況を改善するために、我々はブロックチェーン技術の分散型の特徴を使用して世界中で AI マシンのコンピューティングパワーの借りや配布を行います。ブロックチェーン暗号化技術は、効果的に内部リークの問題を回避できます。また AI および分散コンピューティングユニットのメンテナンスを人工知能コンピューティングユニットのオーナーに引き渡すことでメンテナンスの負担が軽減されます。この全体目標は、以下の副目標に分割することができます。

1. シェア AI コンピューティングプラットフォーム

シェア AI コンピューティングデバイスプラットフォームは、需要状況 AI デバイスのオーナーとユーザーの間のアンバランスの問題を解決します。AI コンピューティングデバイスのユーザーが 100%のコンピューティングパワーを発揮できないため、コンピューティングリソースの一部の閑散を引き起こしました。同時に、多くのユーザーは、人工知能コンピューティングパワーが必要ですが、経済的な AI コンピューティングリソースを得られません。ブロックチェーン技術により、ピアツーピアの支払いやブロックチェーン台帳記録技術がシェア AI コンピューティングを、最も便利な方法で支払いと共有を実現できます。

2. AI 物理コンピューティングユニット

GPU コンピューティングマイニングマシンの多くは、AI コンピューティングタスクに変換でき、単純なハッシュコンピューティングからより意味のある AI コンピューティングタスクに変換することができます。 AI コンピューティングの特殊性のために、あらかじめ指定されたシステムを設置し、定期的にクライアントや台帳記録システムを更新しなければ、ハードウェアや AI コンピューティングのパワーを十分に発揮するができません

3. 分散型 AI アプリケーション

分散型 AI アプリケーション（Decentralized AI Application）がシステムに接続するのに SDK、API が必要です。これに基づき開発者は容易にシステムの強力なコンピューティングパワーを利用できます。主に支払い API、コンピューティングパワー見積り API、ワークロード見積り API などが含まれます。

4. 統合された IPFS 分散型ストレージ

分散型アプリケーションでは、ファイルストレージシステムを使用してデータを貯蔵する必要があります。従来の集中型クラウドストレージまたはローカルファイルストレージを IPFS ストレージシステムに置き換えれば、よりよい分散型ストレージを実現できます。

IPFS （Inter Planetary File System）は、永続的で分散型ストレージと共有ファイルを作成するために設計されたネットワーク転送プロトコルです。コンテンツアドレス指定可能なピアツーピアハイパーメディア配信プロトコルです。IPFS ネットワークのノードは分散型ファイルシステムを構成します[2]。将来の IPFS のほとんどは、クロスチェーンテクノロジコールを使用します。インターチェーンテクノロジについては、インターチェーンサービスコールを参照してください。

5. AI エンジニア育成センター

NebulaAI は人工知能育成センターを設立し、人工知能の実践に関する基本的な知識を提供します。エンジニアは、全般的学習やプロジェクトの実用的な操作を通じて、徐々に製品デザインにおいて人工知能モデルを確立し、訓練します。われわれは、人工知能産業における最新のアプリケーションと知識を普及させ、優れた人工知能の人材を育成することに全力を注いでいます。人材不足を解消し、ビジネスにおける人工知能の力を最大限に発揮することを使命にしています。

6. 10MW 人工知能センター

AI コンピューティングセンターが Nebula AI に大量のコンピューティングパワーと初期実験の場面を提供する予定です。Nebula AI の開発に伴い、大規模な人工知能アプリケーションは、アプリケーションをテストするための研究施設と 51%攻撃への保護が必要となります。

2　NBAI 生態システム

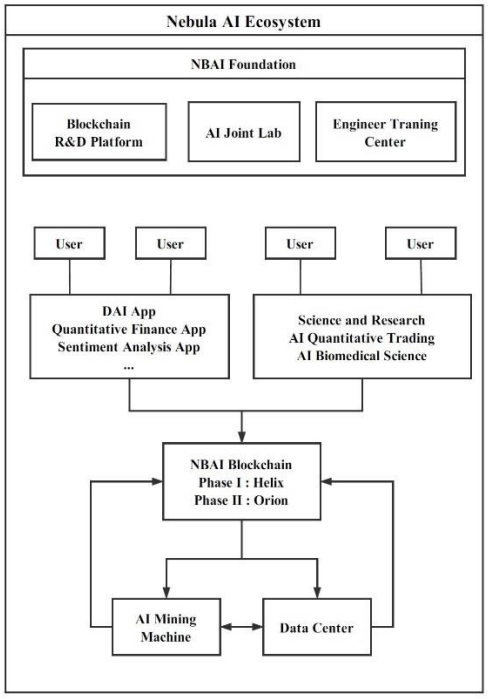

図 1：NBAI 生態システム

NBAI 生態システムは主に NBAI 財団と NBAI システムという 2 つの部分で構成されています。 NBAI 財団はブロックチェーンの R&D プラットフォーム、人工知能連合研究室及びエンジニア育成センターの発展と運用管理をサポートしています。NBAI システムは DAI App、科学研究アプリケーションや大学教育などトップレベルのアプリケーションと NBAI ブロックチェーンや人工知能マイニングマシンや人工知能データセンターなどの基礎サポートを集合しました。

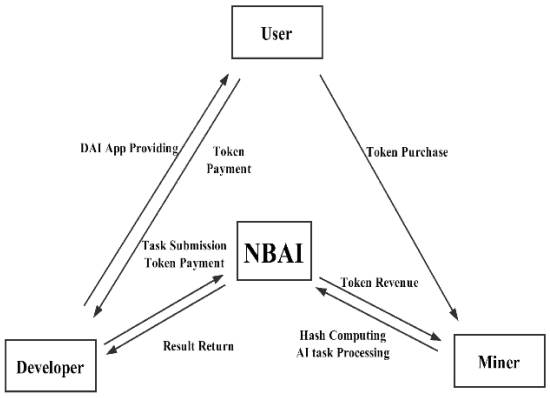

図 2：経済モデル

NBAI 生態システムの経済モデルを図 2 で示します。開発者は DAI App をユーザーに提供し、ユーザーは NBAI トークンを支払うか、開発者のルールに従ってアプリケーションを無料に使用します。開発者は、NBAI に人工知能タスクを提出し、NBAI が推定した費用を支払います。支払が完了後、NBAI がタスクを公開し、マイナーが自由にタスクを受け取り、完了後トークンを取得します。ユーザーとマイナーは取引所を通じて NBAI トークンを交換することができ、以上のように、完全な付加価値を増加する経済モデルを実現しました。

2.1 NBAI

NBAI システムでは、多くの人工知能の深度学習モデル（RNN、CNN、LSTM）が存在しており、トレーニングを実現させるには、多くの GPU コンピューティングが必要です。この問題を解決するために、我々はブロックチェーンマイニングパターンを変更し、PoW だけではなく早期 PoW と後期 PoG（Proof of Group) を使用して、トークンを発行します。既存のマイニングマシンは、人工知能コンピューティングを行ってトークンを得ることができます。初期には、ブロックの安定性を確保するために、ワークロード証明（PoW）を使用されますが、中期的にはグループの作業証明（PoG）を使用します。

2.1.1 Helix (PoW)

ホワイトペーパーが発表されると同時に、スマートコントラクトを読み込む人工知能のパブリックチェーンがリリースされることになります。そのため、プロジェクトの第 1 段階では独立な ether チェーンが使用されます。以下のメリットがあります。

- トラフィックの遅延は比較的に少ないです。
- ガスは自己定義できます。マイナーがスマートコントラクトのガス収入に頼るのではなく、スマートコントラクトを通じて収益を稼ぐよう促す。
- 難易度は自己定義できます。ブロック生成の速度を上げ、トークンの生産速度を調整します。

各人工知能ノードは、異なるコンピューティングパワーによってスマートコ

ントラクトを介してタスクプール内のタスクをコンピューティングし、結果を提出した後に報酬のトークンを受け取ります。スマートコントラクトのハッシュがブロックに記録され、タスクのアドレスが識別されます。タスクアドレスとワークロード、および作業コストは、コントラクトで設定されます。

しかし、ビットコインは、世界のコンピューティングパワーのほとんどを集めており、他の PoW は独自の安全を保護するために十分なコンピューティングパワーを得ることが困難となりました。マイニングは資源の浪費を引き起こし、環境破壊やエネルギー不足につながり、人々の負担になります。ブロックの確認時間を短縮することは困難で、コンセンサスメカニズムに到達するには比較的長い期間がかかり、現在の流行のビジネスアプリケーションに適していません。また、PoW はバランスの取れた攻撃を解決する方法がありません[7]。要するに、我々は NBAI 生態システムは PoW の潜在的な問題を解決し、NBAI のコンセンサスメカニズムを最適化にするために新しいコンセンサスメカニズムが必要だと信じています。

2.1.2 Orion (PoG)

人工知能のトレーニングデータが非常に大きいので、システムのデータを得る時間が非常に重要である。クラウドコンピューティングの特性として、通信ノードの間の距離が近ければ近いほどコストが低く、対応するコンピューティングの効率が高いです。この特徴に基づいて、PoW コンセンサスメカニズムの既存問題を考慮し、PoG を使用します。 PoG では、コンセンサス・システムと NBAI トラストメカニズムを使用して、効率とセキュリティを確保します。

以下のように定義します：

定義 1　ワークノードとマスターノード

ワークノードは、主な人工知能コンピューティングタスクを実行するノードであり、その主な役割は、スマートコンピューティングタスクです。

マスターノードは、通常のコンピューティング機能に加えて、他のノードを管理したり記帳機能を担当したりすることもできます。 AI タスクが分散実行を必要とする場合には、マスターノードは、タスクを実行するために、すべての地域のノードにタスクを割り当て、結果を IPFS に書き込みます。また、遂行したタスクをビザンチンコンセンセスを通じてチェーンに提出し検証しま

す。

新しいワークノードがシステムに参加する時、まず周辺ノードにブロードキャストします。

- 周囲のノードの応答時間が時間 t 以内であることが分かる場合

周辺ノードネットワークへ参加し、ワーカーの 1 つになります。

- 時間 t 内に返事がない場合

自身がマスターノードになります

定義 2　マスターノードになる方法

ノードネットワークでは、ワークノードがマスターノードになる方法が 2 つあります。

- ネットワーク内の元のプライマリノードが消えた場合、最高のクレジットを持つノードが自動的にマスターノードになります。
- ネットワークにワークノードが n 個存在し（P と記す）、生存時間は t であると仮定すれば、もし∃pi と他のノードの応答時間の総数∑n−1 T とその自身の生存時間 ti の積が最小のであればそのノードがマスターノードになります。

定義 3 仮想ワークグループ

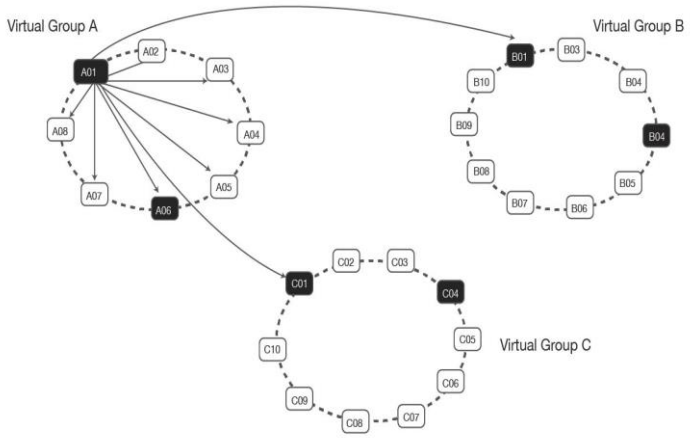

図 3：仮想ワークグループ

いくつかの作業ノードが作業グループを合成します。バックアップ係数は、ノードのワークグループは、同時にノードにおける N のノードがあると仮定すると、会計処理することができるように、バックアップ因子 1 <K <N + 1 であってもよい定義されています。時に、K = N、ヘリックスにシステム。バックアップシステムは、グループ内の台帳を保管する方法です。しかし、人為的裏付け試み k の係数を増加させることによって、収入を得ることを試みるため

に、このシステムは、AI コンピューティングから主な収入をもらうように設計され、マイニング収入は AI ノードコンピューティング 収入より低いです。

定義 4 グループ間の通信

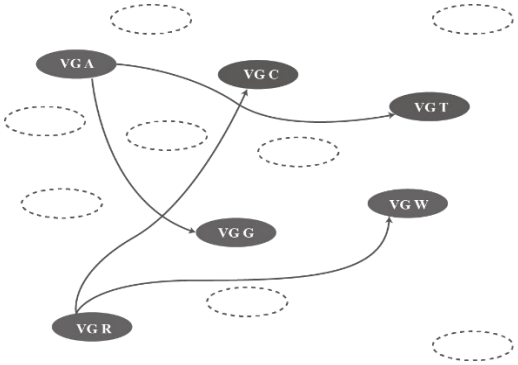

図 4：グループ間の通信

ワーキンググループは、共通記帳ネットワークを形成します。共同記帳のためにビザンチンコンセンサスシステムを使用します[10]。51%の攻撃と記帳効率のバランスを充分に保証します。

Nebula AI によって提案されたグループ作業（PoG）の証拠では、Pi と表される各参加者は、ブロックチェーンネットワークにおいて、彼が重要であると考える他の人々（Pkj）を知る必要があります。取引は T S として記録され、グループ内の他の多数の人々が以前の取引に一致するのを待つ必要があります。

Pi、P kj グループ G、コンセンサスアルゴリズム Consensus（A、B）、コンセンサス検証アルゴリズム V erify（V、NL）を仮定すると、各ノードのコンセンサスは次のようにコンピューティングされます。

$$\forall i \quad TS(P_i) = \prod_{j=1}^{n} Consensus(Pk_j, P_i) \tag{1}$$

さらに、重要とみなされる参加者は、重要な参加者が同意した場合にのみ認識されるなど、ワークグループでは、最終のコンセンサスコンピューティングは次のとおりです。

$$TSA = Verify(\frac{\prod_{i=1}^{n} TS(P_i)}{Consensus(G)}, [P_i, Pk_j]), \quad P_i \in G \cap Pk_j \in G \tag{2}$$

最後に、ネットワークノードが十分ある場合、システムはこの取引を受け入れ、この一連の階層化されたグループコンセンサスにより、攻撃者は完全な合

意情報を得ることが不可能になり、攻撃できなくなります。このようにして、参加者は取引の入力を検討します。 PoG コンセンサスは、人工知能タスクおよび取引情報の完全性を確保することができます。

2.1.3 タスクの実行

タスクプールには 2 つのタスクが含まれています。

- システム生成タスク：例えば、Ethash、蛋白質シーケンシングなど、標準的な単位が返されます。
- ユーザータスク：ユーザーは特定の問題を解決するためにタスクを送信し、タスクリターンを設定します。いずれのタスクでも、契約書とコンピューティング結果を提出するためのスマートなプロトコルシステムが付加されます。マイナーは、タスク報酬と記帳報酬両方が獲得できます。

一つの標準のトレーニングタスクには、次のものが含まれます。

- ミッションのためのトレーニングデータ：データセットは foundation またはカスタマイズから得られます。
- タスクが使用するトレーニングスクリプト：トレーニング方法は、標準の深層学習モデル（RNN、CNN、LSTM など）およびその他のカスタムメソッドを使用します。
- トレーニング報酬：トレーニング作業は AI マイニングマシンで完了し、報酬額を指定する必要があります。高い費用で訓練の優先度を高めることができます。

タスクシステムは IPFS に貯蔵され、暗号化されたアルゴリズムコードとタスクコードが含まれます。マイニングマシンがコンピューティングタスクを受け入れると、独自のハードウェアパラメータを返し、コンピューティングタスクユニットとトレーニングデータセットをリモートからダウンロードします。標準の Distributed TensorFlow がカプセル化された後、適切な冗長コンピューティングが追加され、コンピューティング結果の信頼性が保証されます。

2.1.4 チェーンインターオペラビリティ

分散型の人工知能システムとして、多くのコンポーネントが分散型ですが、すべての自己設計型開発は非常に非効率的です。システムは他の分散サービスと接続し、チェーン全体で簡単に使用できます。クロスチェインには 2 つのタ

イプがあり、バリューチェーンインターとテクノロジーチェーンインターです。

バリューチェーンインターは分散型の交換所によってチェーンインター取引が実現されます。例えば EtherDelta でスマートコントラクト取引を通じて対応するサービスのトークンをもらい、トークンでサービスを実現します。その技術が簡単で運用しやすいですが、性能が低いです。しかし、サービスに必要なトークンの交換がシステム内で進められれば、遅延を減らすことができます。現在の状況下では、USDT とビットコインは典型的な価値のチェーンインターメディアになります。

テクノロジーチェーンインターの事例として、Bitcoin と Litecoin の間のチェーンインターアトミック取引があり、Segwit の隔離証拠を通じて異なる通貨間でチェーンインター取引が実行されます。ほかに、ZCash とイーサリアムはゼロ知識検証取引を実行しています。、Zcash ブロックチェーンではゼロ知識証明を使いプライベート取引を作成するため、Zcash トークンを追跡することができません。基礎チェーンは、チェーンインター取引に対応する必要があり、もはや多くの ICO プロジェクトがチェーンインターを試みています。例えば、Ethereum はチェーンインター通信の分野で Polkadot プロジェクトを打ち出しました。この設計のコアコンセプトは、2 つの主要なブロックチェーンテクノロジトランスミッションとアクセプタンスの問題を解決することです。このプロジェクトは現在、Ethereum に焦点を当て、私設チェーンとの相互接続を実現し、他のパブリックチェーンネットワークとのアップグレードを実現します。その技術が成熟した後の目標は、プロジェクトの範囲と性能を大幅に向上させることです[5]。

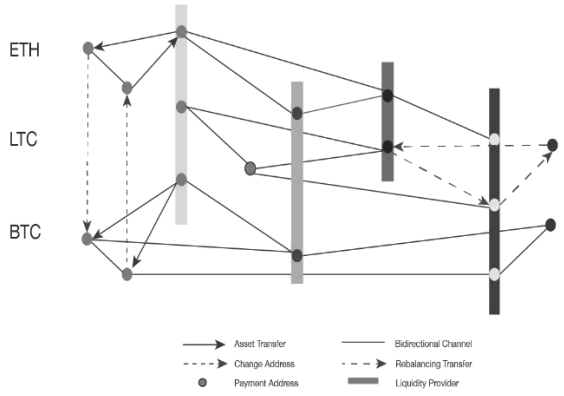

図 5：チェーンインターオペラビリティ

2.2　人工知能データセンターとマイニングマシン

2.2.1　人工知能データセンター

大規模なユーザーが参加する前に特定の AI コンピューティングの供給を保証するために、我々はケベック州におけるマイニングセンターで、初期コンピューティング能力を提供します。 ケベック州で消費電力 10MW のコンピューティングセンターを建設しています。 ケベックは、世界的に競争力のある電気料金、寒い気候、十分な人材を持っており、34 個のデータセンターがここに位置しています。さらに、IBM、Nokia、Amazon、Microsoft を含む世界的に有名な大手企業がここにデータセンタールームを建設しました。

人工知能データセンターとしてケベックの利点：

- 豊富な水資源と低い電気料金。

表 1：ケベックの電気料金

Province	375 kWh	750 kWh	1,000 kWh	2,000 kWh	5,000 kWh
Quebec	32.48	52.77	68.66	146.46	379.86
Manitoba	34.03	60.96	78.92	150.75	366.24
British Columbia	32.05	61.92	89.07	197.63	523.34
New Brunswick	52.88	88.32	111.94	206.44	489.94
Alberta	57.775	96.175	121.78	224.195	531.44
Saskatchewan	61.955	103.685	131.505	242.79	576.65
Ontario	64.7	110.64	141.69	267.34	674.38
Nova Scotia	64.69	118.55	154.46	298.09	728.98

Ontario Hydro 2013 年の統計によると、カナダはの電気料金は世界でもっとも安いです。カナダのすべての州の中で、ケベック州の電気料金が最も低く、90%以上が水力エネルギーを使用しています。

- 比較的な低気温

ケベック州の一年の九か月は冬であり、平均気温はマイナス 10 度以下です。また、夏になっても平均気温は 20 度未満です。

- 十分の人材

Google、Facebook、Microsoft はすべてモントリオールに人工知能センターを設置しています。ここは、人工知能の人材を多くを集めます。例えば、モン

トリオール大学コンピュータサイエンスおよびオペレーションズ・リサーチ学部のヨシュア・ベンジオ（Yoshua Bengio）教授は、人工知能の領域の世界トップの教授です。彼はアルゴリズムを研究するモントリオール研究所３人の創設者の一人です。

また、カナダ政府は人工知能の研究開発を完全にサポートしています。連邦政府は、モンペリエ大学に 21 億 3000 万ドルの特別助成金を付与しており、州政府は今後 5 年間でさらに 1 億カナダドルを投資する予定です。

- Nebula AI は、世界トップレベルの大学である McGill 大学医学院と協力して、AI に関する共同研究協力を進め、外科における人工知能の革新的アプリケーションの研究に取り組んでいきます。

2.2.2 人工知能データセンターマイニングマシン

1 つの 1080Ti グラフィックスカードは、7514 GFLOP / s のコンピューティング能力を備えています。 GTX 1080Ti で Caffe 枠組みを使うフレームワークは 130 万の画像データの GoogLeNet モデルを訓練し、19 時間 43 分に 30 回反復します。6 枚のカードの並列コンピューティング時間は 3.5 時間に短縮できます。

いかなる CUDA 操作（主に Nvidia シリーズグラフィックスカード）をサポートする GPU マイナーは、AI マイニングシステムをインストールできます。など TensorFlow、などの一般的な AI 人工知能など CNN、RNN、DNN としてマイニングマシンのアルゴリズムだけでなく、他の一般的に使用されるライブラリの数、プリロード、システムが自動的に事前に AI をサポートするためのライブラリを更新することができ、アップグレードのクライアントが付属しています。 miner の最初のバッチは、主に Python 3.6 サポートライブラリをプリロードします。 Ethash 対応の記帳クライアントもシステムに統合されています。

AI マイナーは 3 種類の収入がもらえます：

- 記帳コンピューティング収入

Equahash ベースのアルゴリズムは、記帳部分の収益をサポートします。しかし、所得のこの部分は、一般に AI のコンピューティングされた収入よりも少ないです。

- AI コンピューティングによる収入

AI コンピューティングによる収入はマイナーにとって最も重要な収入源です。

- IPFS 収益

マイナーはダブル掘削モードを設定することができ、Sia、storj タイプのファイル共有通貨をマイニングできます。 IPFS は、AI コンピューティングに格納されたデータの支払いにも使用できます。

2.3 DAI App 開発

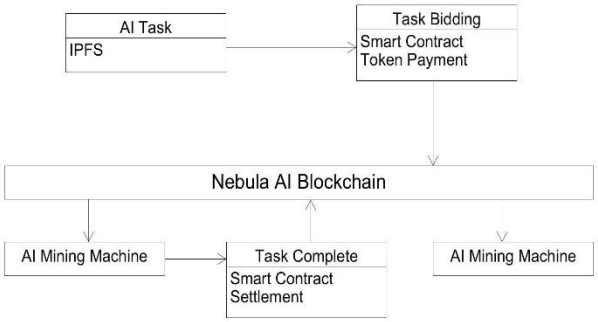

図 6：人工知能 DAIApp

Ethereum コミュニティは、スマートコントラクトに基づくアプリケーションを DAPP といいます。DApp の設計目標は、スマートコントラクトのためのフレンドリーなインターフェースと、IPFS などの追加機能を持つことです。DApp は、Ethereum ノードとやりとりできる集中サーバー上で実行できます。たとえば、有名な etherdelta、ether cat などです。

しかし、分散型人工知能アプリケーション（DAI App）では、スマートコントラクトだけでは不十分です。その理由は次のとおりです。

- Ethereum スマートコントラクトには、人工知能のコンピューティング機能がありません。

EVM は Turing-complete 仮想マシンですが、そのコンセンサスコンピューティングシステムは単純なタスクしか実行できず、複雑な人工知能コンピューティングを実行することはできません。

- Ethereum のマイニングクライアントには、人工知能のコンピューティングに必要なコンピューティングライブラリをサポートしません。

人工知能の運行は、主に様々な開発パッケージのサポートに依存し、分散型コンピューティングがその主要タスクです。関連するコンピューティングタスクに必要なサポートライブラリは、別々のコンピューティングクライアントで実装できます。

しかし、商用の人工知能アプリケーションとして、ブロックチェーンのスーパーブックと支払い機能は、依然としてシステムの中核です。人工知能コンピューティングリソースの不足のために、コンピューティング能力の共有は非常に便利な機能となります。各ユーザーはチェーンにリンクし、ブロックチェーン貸出コンピューティング機能を使用してコンピューティングタスクを完成させることができます。各 DAI App 開発者は、自分のニーズに合わせて標準に準拠したスマートコントラクトを作成できます。

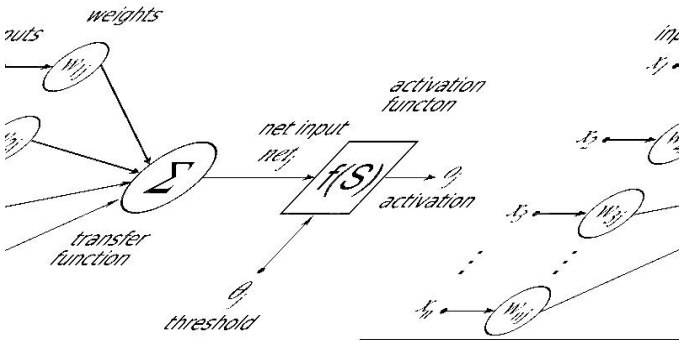

図 7：深層学習

深層学習モデルを訓練する場合、順方向パスと逆方向パスの 2 つの主要な操作が実行されます。順方向パスでは、入力がニューラルネットワークを通じて、入力が処理された後に出力が生成されます。逆送信では、ニューラルネットワークの割合は、フォワードエラーに基づいて更新する必要があります。ニューラルネットワーク訓練では、最も重要な問題の 1 つが訓練速度であり、特に深度学習の場合、パラメータの調整は多くの時間を消耗します。ニューラルネットワークコンピューティング集約部分は、複数の行列アルゴリズムで組み合わせ、GPU が行列演算や数値コンピューティングにおいて独特な優位性があり、特に浮動小数点、並列コンピューティング性能が CPU の数十か数百倍優れており、マトリックスと数値コンピューティングの点で独特の利点を有しています。学習モデルの深さは、GPU を使用して訓練すると低消費電力化の場合には、フロントをサポートするためのインフラ未満を占有し、データスループット大量のように、それは、クラウドに分類し、予測を容易にすることができま

す。したがって、スマートコントラクトによる人工知能コンピューティングを実行するのに十分なコンピューティング能力を得ることは有効な手段です。

我々は典型的なスタイル深層学習伝達モデル（Gatys et al.）を例にして、GTX 1080Ti GPU、K80 GPU（AWS P2）、i5 7500 CPU 及び CPU（AWS P2）は tensorflow 枠組みのコンピューティングを使用して比較します。

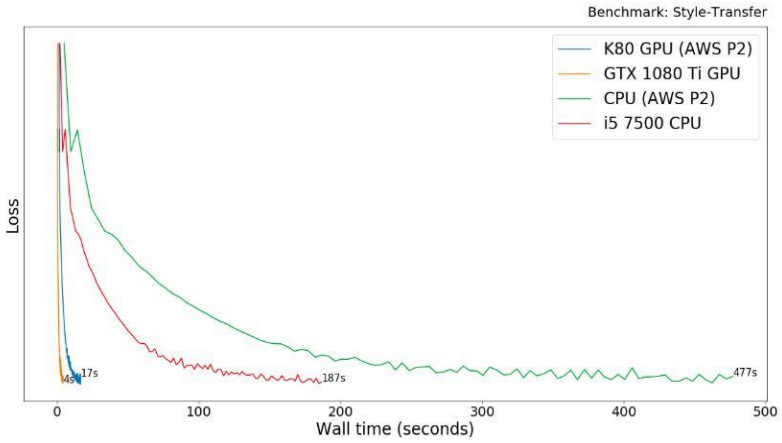

図 8：速度の比較

GTX 1080 Ti GPU の性能は、i5 7500 CPU の性能よりも 50 倍近く優れています。

NebulaAI は非常に競争力のあるコンピューティングパワーを提供します。Nvidia の 1080 チタンを使用した NebulaAI 人工知能のマイニングマシンは、Amazon P2.xlarge instance（Nvidia Tesla K80）で、例えば私たちは、次のコンピューティングを行い、Nvidia の 1080Ti の価格が 1000 カナダドルで、電気の時間あたりの価格は 0.1 カナダドルを消費し、仮に 1080Ti の寿命は 2 年であり、1 時間当たりの単価は 1000 /（36×2×24）+ 0.1 = 0.157 カナダドル/時であります。

公式テストデータを通じて、Nvidia 1080 Ti の Tensorflow GPU 性能が Amazon P2.xlarge instance の 4 倍であり[14]、P2.xlarge 価格は 0.9 カナダドル/時であり、NebulaAI のコンピューティングパワーの単価の 23 倍です。ユーザーはコンピューティングのために Amazon サーバーにデータをアップロードする必要がありますが、データの私有を保証することができません。分散型の NBAI を使用することでこの問題を解決できます。

2.4　大学教育

NBAIは世界の各主要な大学の科学技術コンピューティングに豊富なインターフェイスを提供します。これにより研究者の研究効率を大幅に向上させ、科学開発のコストを削減し、クロスポーだー、多領域且高級なプログラミングの需要と基礎配置を結び合うことができます。NBAI が提供した PaaS（Platform as a Service）を利用することで、学生は興味分野の学習にさらに集中することができます。

2.5 Nebula AI 財団

Nebula AI システムは NBAI 仮想通貨を使うパートナーコミュニティーを作ろうとしています。このコミュニティーのメンバーに向けて、Nebula AI 財団は独立・非営利・民主的な管理機関となることを目指しています。

Nebula AI 財団の目的は AI ベースチェーンの宣伝・教育および起業支援です。コミュニティーへの参加は励まされます。同時に、いかなる組織がシステムを Nebula AI のプラットフォームに統合し、DAI アプリを開発することは歓迎されます。

独立性の原則に基づいて、Nebula AI 財団のウォレットが 3/4 マルチ署名を使います。署名を増えたい場合、財務および人事管理委員会の許可が必要です。大部分のトークンがコールドストレージで保管され、ほかのトークンがマルチ署名で保管されます。

2.5.1　人工知能協力研究室

Nebula AI 財団が AI・ブロックチェーン・分散型計算などの分野においてモントリオール大学、トロント大学、マギル大学と協力します。カナダ政府はトロントとワーテルロー、モントリオール、エドモントンでスーパー人工知能センターを設置し、資金・業務・人的資源の完備している環境を造る予定です。2017 年の予算表によると、予算は上記の地域の人工知能産業に集中します。これは国のレベルで人工知能が最優先になったということ表しています。

モントリオール大学の Yoshua Bengio 教授と彼のチームが過去 10 年で研究を進め、良い基礎を築き上げ、モントリオールを人工知能の前線に推し進めま

した。Bengio 教授がモントリオール大学のアルゴリズム研究所（MILA）で学術研究をしています。MILA が IVADO という研究所に支持されています。現在、Nebula AI が積極的に MILA と交流し、研究開発を進めていきます。

北アメリカのトップ医学院であるマギル大学の外科イノベーションプロジェクト（Surgical Innovation program）のチームが、Nebula AI と一緒に AI 医学映像分野の研究を進めています。この研究は Mitacs プロジェクトによって支持されています。Mitacs プロジェクトはカナダ情報技術と総合系統数学組織（Canadian Information Technology and Integrated Systems Mathematics Organization）によって設立されたプロジェクトで、10 年あまり運営されています。有名な Jake Barralet 医学教授が Mitacs プロジェクトのリーダーを務めています。

2018 年 2 月、Nebula AI がシリコンバレーで研究室を設け、ローカルな大学や業界と手を組み、人工知能の応用およびブロックチェーンの研究を行っています。

2.5.2 ブロックチェーン開発プラットフォーム

Nebula AI が構築するブロックチェーンの研究開発プラットフォームは Nebula AI ブロックチェーンエンジニアとコミュニティーの貢献者を中核として、大学や業界と協力します。それと同時に、ブロックチェーンエンジニア養成センターに技術サポートと人材を提供します。

Nebula AI の研究開発プラットフォームは以下の内容を開発しています：サンプル、API・SDK の接点、オンライン学習ビデオなど。プラットフォームには技術サポートチームとシナリオ実施センターが設けられています。世界各国の開発者とコミュニティーの協力者が絶えずに Nebula AI の研究開発プラットフォームの機能を高めています。

2.5.3 人工知能及びブロックチェーンエンジニア育成センター

どのプロジェクトにも大勢のエンジニアは必要ですが、現在では人工知能のエンジニアが足りていません。Nebula AI は資金で協力し、あるいはプロジェクトのプラットフォームとしてローカルな ECV learning などの教育機構と協力します。Nebula AI の科学者たちは講師として、大勢の AI 実習生を雇用し、絶えずに人工知能産業に優れた人材を提供します。2018 年 1 月 27 日、熊騰科

博士の AI エンジニア養成プロジェクトが始まりました。数多くの学員が来て、将来 Nebula AI の開発チームの予備力になります。ブロックチェーンエンジニア養成プロジェクトも 2 月の中旬から始まりました。

3　NBAI ストラクチャデザイン

3.1　NBAI ロジックストラクチャ

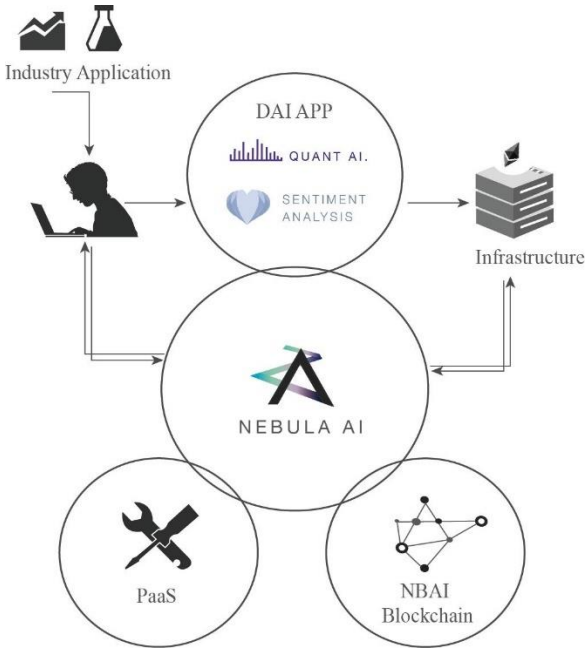

図 9　システムのロジック

NBAI のロジックアーキテクチャは主に業界アプリケーションへのニーズと開発者・DAI App・インフラ・Nebula AI との交流に構成されます。その中に Nebula AI が PaaS (Platform as a Service)と NBAI ブロックチェーンを提供します。金融、医療、生物などの業界からの人工知能開発ニーズは多くあり、開発者が各業界の応用場面に応じて DAI App を開発する必要があります。アプリの配備と Nebula AI の生態システムに加入することでソリューションを提供し、収入をもらいます。開発者が簡単に使用できるように、Nebula AI は数多くの接点とアプリケーションを提供します。NBAI の分散型ブロックチェーンは Nebula AI のクレジットメカニズムと合わせて、P2P トラストとビッグデータ処理の効率問題を解決する予定です。

3.2　NBAI システムストラクチャ

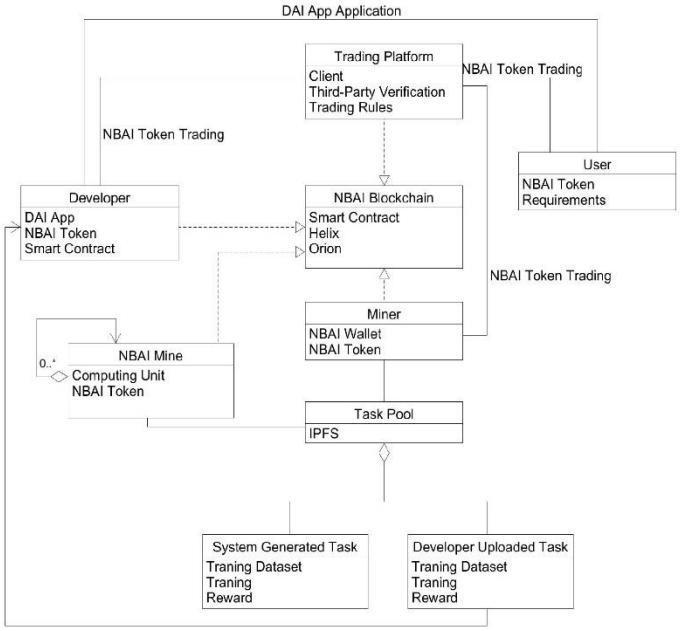

図 11 システムアーキテクチャ

上の図が示したように、NBAI のシステムアーキテクチャが主に NBAI、開発者、ユーザー、取引センター、マイナー、タスクプールに構成されます。NBAI は分散型の NBAI ブロックチェーンを提供するだけではなく、NBAI トークンの取引センターも提供します。これで NBAI エコシステムにおける価値の交換を強化します。

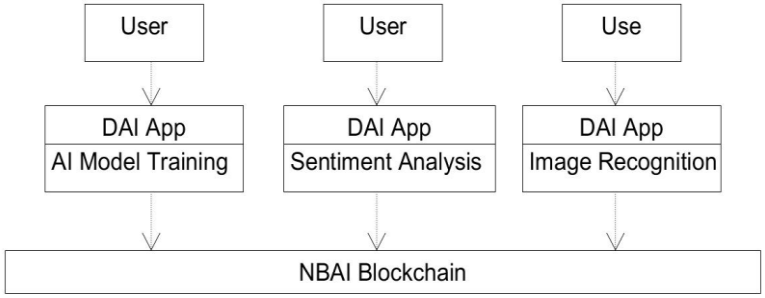

図 11　共有した AI クラウドコンピューティングプラットフォーム

Nebula AI が共有した AI クラウドコンピューティングプラットフォームを提供しています。PaaS (Platform as a Service)があれば、IT 業界以外の人でも速やかに開発できます。こうしてシステムとコンピューティング能力への依存が弱くなります。

3.3　API/SDK サポート

前払いや費用を追加するスマートコンタクトは SDK で接点を自動的に形成できます。API を使えば、ある集中型のサービスに接点を提供できます。SDK がサポートするのはまず python を主要なプログラミング言語としているもので、その後 java や.net もサポートします。

SDK のサポートがあれば、ユーザーは簡単に AI コンピューティングを使えるようなになります。SDK は便利であると同時に、ユーザーと集中型システムとの間の接点にもなります。

4　NBAI 最適化デザイン

4.1　データ安全の暗号化

データは準同型暗号で暗号化し保存されます。準同型暗号とは、いくつかの暗号化されたデータを計算した後に解読し、その結果は暗号化される前のデータの計算結果と一致しているということです。現在の準同型暗号ソリューションは部分的準同型暗号（partially homomorphism）、軽度準同型暗号（somewhat homomorphism）、完全準同型暗号（fully homomorphism）という三種類に分けられます。部分的準同型暗号は一種の代数演算（掛け算、足し算など）だけ実行できます。軽度準同型暗号はある回数の掛け算や足し算を同時に実行できます。完全準同型暗号は掛け算や足し算を何度も実行できます。準同型暗号はデータを暗号化することだけではなく、暗号文の計算においても実行できます。
$<G, *>$と$<H, o>$が二つの代数系で、$f : G \to H$がマッピングと仮設します。全ての If $\forall a, b \in G$ にとって、$f(a * b) = f(a) of(b)$ が成立する場合、f は G から H までの準同型暗号だと言えます。暗号化は平文から暗号文のマッピングです。もし暗号化されたマッピングが準同型マッピングであれば、この暗号化の方法は準同型暗号アルゴリズムと呼びます。言い換えると、準同型暗号は暗号化計算と代数演算の順を変えられるアルゴリズムです[20]。定義は以下のようです。

E(K,x) は暗号化アルゴリズム E とキーK で x を暗号化すると仮設します。F はある種の演算を表します。もし暗号化アルゴリズム E と演算 F にとって有効なアルゴリズム G があり、

$$E = (K, F(x1, ..., xn)) = G(K, F, (E(x1, ..., xn))) \quad (3)$$

が成立すれば、暗号化アルゴリズム E は演算 F の準同型とします。

もし上記の数式が $F(x1, ..., xn) = \sum_{i=1}^{n} x_i$ だけの場合で成立すれば、この暗号化アルゴリズムは足し算準同型暗号アルゴリズムです。

もし上記の数式が $F(x1, ..., xn) = \prod_{i=1}^{n} x_i$ だけの場合で成立すれば、この暗号化アルゴリズムは掛け算準同型暗号アルゴリズムです。

もし上記の数式が足し算や掛け算を含む F (x1, ..., xn) の場合で成立すれば、この暗号化アルゴリズムは完全準同型暗号アルゴリズムです。一種の演算で成立するのは部分的準同型暗号です。

公開鍵システムの準同型暗号アルゴリズムεは KeyGenε と Encryptε、Decryptε

という三つの部分に構成されます。

KeyGenε：安全係数 λ を入力すると、私有鍵としての sk と公開鍵としての pk を出力します。pk は平文空間の P と暗号文空間の X を定義します。

Encryptε：pk と平文 π∈ P を入力すると、公開鍵の pk で平文 π を暗号化さした暗号文 ψ ∈ X を出力します。ψ = Encryptε(pk, π)で表します

Decryptε：sk と ψ を入力すると、平文 π を出力します。

上記の 3 つのアルゴリズムの複雑さは λ の数式によって決めます。暗号化システムは以下の条件を満たせなければなりません：もし(sk,pk)■(R@←)〖KeyGen〗_ε (λ)、かつ π∈ P、ψ■(R@←)〖Encrypt〗_ε (pk,π)が成立すれば、〖Decrypt〗_ε (sk,ψ)= π。

そのほかに、Encryptε というアルゴリズムがこのように解釈されます：公開鍵としての pk、集合 Cε から取り出された一つの C、暗号文 Y =< ψ1, ..., ψt >を入力し、暗号文 ψ ∈ C を出力します。もし
ψi = Evaluateε(pk, πi), i = 1, ..., t,が成立すれば、

$$\text{Evaluate}\varepsilon(pk, Y, C) = \text{Evaluate}\varepsilon(pk, C(\pi 1, ..., \pi(t)) \quad (4)$$

が成立します。

演算方法が保存されたら、データのアーキテクチャも保存されます。従って、機械学習のプロセスにおいて、データのアーキテクチャだけあれば、暗号化された情報の解読と機械学習を行えます。

4.2 分散型システム最適化

データ伝送はビッグデータの平均分割処理によって加速されることができます。NBAI のノードがタスクを受け取って同時処理し、その結果が選ばれたノードに戻ります。その後はタスクの合併を行います。最後の結果はタスクの所有者のところに戻ります。データの伝達と処理のプロセスにおいて、ノードの選出、データのアクセス、負荷分散、ネットワークの安全、冗長性の研究などを通じて NBAI を最適化します。

NBAI は開発者からビッグデータレベルの人工知能タスクを受け取った後、一人のマイナーが処理できないので、タスクを分割し複数のマイナーに配分して計算する必要があります。それらの結果を合併し最終結果として開発者に戻ります。この一連の操作は完備かつ最適化した分散型システムに依存します。NBAI も高いスループット、低遅延、強い並行性などの要求を満たせるために

最適化します。

伝統的な分散型システムは三層構造ですが、タスクによって、複層にデザインされる場合が多いです。複層構造には様々なプロキシやルーティングがあります。これらのプロキシプロセスの間に、多くのアプリケーションは TCP を通じて前後を結んでいます。しかし、TCP の故障率が高くて、メンテナンスの費用も高いです。従って NBAI はメッセージキューイングメカニズムを利用します。

NBAI は NoSQL を使ってデータ保存層の分布問題を解決します。NoSQL は容量が大きくて、アクセスが速いというメリットを持つと同時に、一つの索引で検索や書き込みしかできません。このような制限のおかげで、システムは索引に従ってデータ保存のプロセスを定義できます。こうしてビッグデータ級のデータは安全に複数のノードに送ることができるようになりました。

```
future<int> get();
futre<> put(int);

void function(){
        get().then(then[] (int i)){
                put(i + 1).then([] {
                        std::cout ”an integer has been put”;
                        });
                });
}
```

図 12 Future/Promise モデル

分散型システムが数多くのネット通信に関わり、非同時性のノンブロッキングプログラミングモデルに依存しているのため、開発者は分散型システムのプログラミングにおいて多くのコールバック関数を生成（generate）します。タスクインストラクションが複数のプロセスに分割され、数回のネット通信で組み合わせて完成します。しかしこのようなやり方はコードのメンテナンスに不利です。従って NBAI は Future/Promise モデルを使ってコールバック関数を最適化します。

5　NBAI トークン

5.1　トークンプラン

5.1.1　トークンの使用価値

トークンを使って計算力を買うことができます。トレーニングのデータが少ない時、消耗されたトークンも少ないです。データが多くなると、消耗されたトークンも多くなります。費用はトレーニングのコストとトークンの現在価値に関わります。トークンの現在価値とは、一つの 1080Ti グラフィックカードが 1 分間の計算力で、すなわち 7514 GFLOP/s × 60 である。

5.1.2　トークンの応用場面

トークンは以下の三つの場合で使用される予定です。

・ 開発テスト

開発者はテストする時、トークンを消耗してモデルのトレーニングをします。支払ったトークンの数によって、モデルのトレーニング所要時間は 50%、90%減少します。

・ DAI アプリの使用

開発者は DAI App を有料 App に設置する可能性があります。そうするとユーザーは人工知能サービスを使いたい場合、トークンを支払わなければなりません。例えば、このホワイトペーパーに書いている仮想通貨のトレンドを予測する App はこのようなアプリです。

・ DAI トレーニングサービスの購入

ユーザーがトレーニングサービスを使ってより正確なモデルを立てるとき、トレーニング費用の要求が出てくる可能性があります。

5.1.3　ユーザーの応用場面

1. 定量的な取引（Quantitative trading）

定量的な取引は早くから機械で仕事をサポートします。アナリストが様々な定量モデル（quantitative models）を使って、指標を設置し、データの散布を観察

します。すなわち機械を計算機として運用します。最近の機械学習の発展によって、速やかに膨大なデータを分析・予測できるようになり、金融商品のトレンドをより正確に予測できるようになりました。しかしこのようなモデルの計算はたくさんの人工知能計算力が必要です。伝統的なやり方では、取引部門ごとに自分のデータセンターを設ける必要があります。計算力を共有したら、高いメンテナンス費用を節約できて、金融会社も予測そのものに専念できるようになります。

2. 人口知能学習者計画

現在、大学が逐次に人口知能授業を開設しています。こういうトレンドが今後の数年間に続くと考えれます。学生たちが勉強するとき、自分のコンピュータで小さいタスクを実行し、学校の研究室で時間のかかるタスクを実行します。しかし、このような断片化的なタスクはブロックチェーンの計算力で実行できます。コストの低い AI コンピューティングサービスが学生の練習に適しています。

3. 生物医学の人工知能

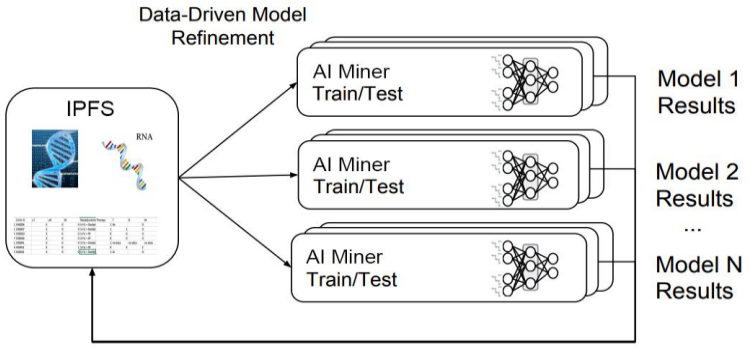

図 13 腫瘍研究向けの AI

腫瘍の早期検査が重大な意義を持っていますが、早期ガンの異常組織が少ないので、伝統的な方法では良性（非がん性）のものか、悪性（がん性）のものか判断しにくいです。医者はよく生検法で検査しますが、コストが高くて、患者さんも辛いです。人口知能を使えば、上記の難題を解決し、医者さんの判断能力を高め、医療サービスの個性化・精確化への転換を促すことができます。

5.2 DAI App 開発者収益モード

1. DAI App のタスク種類

・ I 類 DAI App——モデルトレニーングを必要とする App

この種類の App のユーザーは計算を行うにはトークンを支払わなければなりません。また計算のためにたくさんの資源が消耗されます。レニーングの所要時間はタスクによって数時間から数百時間がかかります。

・ II 類 DAI App——モデルトレニーングの必要がない App、または既存のモデルを使う App

モデルトレニーングの必要がない App は計算力を消耗しないので、一定のスマートコンタクトの費用を支払うだけで、アプリケーションを使用できます。また I 類 DAI App のモデル計算結果を直接引用してもいいです。II 類 DAI App のコストは低いです。

2. コンピューティングタスク

スタンダードな計算力支払うコンタクトは以下の要素を含めます：

AI タスクのデータアドレス

AI タスクのプログラムスクリプト

AI タスクの実行結果の出力アドレス

AI タスクの報酬

3. タスクの公布

タスクがブロックチェーンに発表されたら、全ての AI マイナーはシステムからタスクを受け取ることができます。タスクが実行されたら、「実行中」とマークされます。より正確な結果を得るために、ユーザーはいくつかの冗長性計算レベルを選択できます。異なる冗長性計算レベルに対応するために、Nounce は 1、2、3 などのレベルに設置されることができます。数字が大きければ多いほど、多くの計算が必要です。それに応じて費用も高くなります。

4. 費用の計算

AI 計算はトレーニング段階と使用段階に分けられます。トレーニング段階ではたくさんの資源を消耗し、ほとんどの計算力もこの段階で消耗されます。それに対して、使用段階では、トレーニングが終わったので、必要な計算力は多くないです。タスクが始まるとき、スマートコンタクトはあらかじめ一部の費用を受け取ります。計算が終わったあと、総支出を計算します。ユーザーは残った部分の費用を清算したらデータを手に入れます。

5. タスクの実行

マイニングマシンのクライアントはブロッチェーンからタスクプランを読み取り、実行可能な人口知能コードに解読します。人口知能とトレーニング用の

データは外部のリンクに保存されます。タスクが始まると、以下のスケジュールに従ってコードを実行します。

暗号化したタスクを解読する

データをリモートダウンロードする

タスクを実行状態に設置する

計算の進度と結果を書き込む

報酬を受け取るため、マイニングマシンがアドレスとバインドする

6. 計算の終わり

DApp の使用者は実行結果をダウンロードして、直接に web での展示やオフラインの使用に使えます。また、執行結果は API で受け取ることができ、解読された後使えます。

5.3 NABI AI 応用ケース

ヘッジファンドや銀行、Goldman Sachs のような大手多国籍企業はスマートテクノロジーに基づく外貨と株取引から利益をもらっています。これらの会社はディープラーニングを通じて、金融市場の短期と長期変動を予測します。Pantera Capital などの仮想通貨所有者、サンタンデール銀行、シティバンク銀行などの金融機関も仮想通貨の市場を観察しています。

ディープラーニングモデルのデザイン・構築・トレーニング・最適化のプロセスには、たくさんの計算力が必要です。ユーザーが毎回パラメーターを調整したら、モデルの計算が必要です。この場合、スマートコンタクトで十分な計算力を獲得し人工知能の計算に用いるのは有効な手段ではありませんか。
スタンダートのシステムプロセスは図 14 が示した通りです：

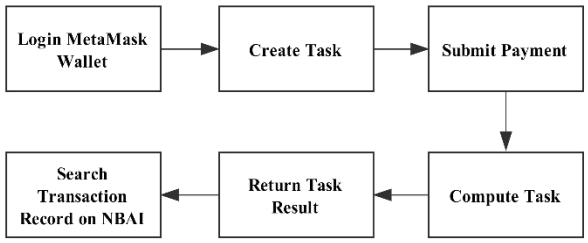

図 14 NBAI AI アプリケース

6　事業計画

Q1 2017　概念の想定、開発の始まり、ハイパーレッジャーの調査研究

Q3 2017　人口知能 DAI APP の開発、概念試作の開発

Q1 2018　トークンの販売開始、
Helix のテストチェーンがサービスイン

Q3 2018　Helix のパブリックチェーンがサービスイン、
初めての DAI APP が統合され；Orion の開発開始

Q1 2019　Orion のテストチェーンがサービスイン

Q3 2019　Orion のパブリックチェーンがサービスイン、
10 の DAI APP を統合する

Q1 2020　Orion に 50 の DAI APP を統合する

Q3 2020　Orion に 500 の DAI APP を統合する

7　協力計画

1.　協力プロジェクト

・　分散型最適化とクラウドコンピューティングプロジェクト

――コンコルディア大学

・ 人口知能外科イノベーションプロジェクト

――マギル大学医学院外科イノベーションセンター& Mitacs

・ カナダ夏インターンシッププロジェクト

――カナダ政府

2.　協力パートナー

モントリオール青年協会

カナダ科学・研究開発基金会

マギル大学

コンコルディア大学

Timechain

Beepay

Express Mining

ECV Learning

JTech Soft

モントリオール IT 協会（APIGM）

8　ICO プラン

初回に発行されたトークンは 67 億で、毎年マイニングによって新しいトークンを産出しますが、その数は 6 年間で毎年 2%から 0.2%まで減らします。ユーザーが人口知能のカスタム予測機能を使うときトークンを消耗します。トークンの使用量は計算量に関わります。システムの正確さの向上により、トークンへのニーズも多くなります。

マイナーはマイニングでトークンを得られます。マイニング報酬の主なリソースは人口知能マイニングマシンです。NBAI トークンは NBAI ブロックチェーンに基づくあらゆるアプリケーションの唯一の仮想通貨です。

トークンは ERC 20 トークンで、未来 NBAI のメインチェーンのトークンによって 1：1 で置き換えられます。

公募の段階では 1 Ethereum = 100,000 NBAI。

私募の開始時間は 2018.1.22 で、終わり時間は 2018.3.30 です。私募段階のソフトキャップは 5,000 Ethereum で、ハードキャップは 18,000 Ethereum です。

公募の開始時間は私募が終わった 1 ヶ月以内です。公募段階のソフトキャップは 10,000 Ethereum で、ハードキャップは 12,000 Ethereum です。

公募段階で未販売のトークンは破壊されます。

45% 私募と公募の段階で販売されます

25% 基金会とコミュニティーが所有

15% コアチームが所有

10% 早期投資家が所有

5% マーケット協力パートナーが所有

基金会所有のトークンはクラウドファンディング終了後凍結されます。その以降 18 の段階（約 3 年間）に分けて解凍します。一つの週期は 60 日間です。毎回解凍したのは基金会所有量の 18 分の 1 です。

公募終了後、逐次に国際のトッププラットフォームでサービスインします。トークン販売の連絡先：tokensale@nebula-ai.com.

9　チーム

9.1　開発チーム

NBAIプロジェクトが2017年の年始から検証され、何回の技術革新を経て、初期のHyperledger Fabricからビットコインに、最後はメインチェーンでイーサリアム（Ethereum）の技術を採用すると決めました。こういう流れで1年間がかかり、アメリカ、中国、シンガポール、カナダなどの国の投資家から投資協力を得ました。

曹滔韜　CEO & Co Founder

2007年复旦大学から卒業、IBM上海などで就職しています。2010年カナダに行き、コンコルディア大学の電子・計算機修士学位を修得しました。同大学で勉強しているとき、NSERC（カナダ自然研究基金）でビデオのトランスコーディングを研究していました。

卒業後カナダのSAP、Autodesk、Expedia、Paysafなどで働き、コアチームのリーダーになりました。

2013年Service ECVictorという会社を開き、ソフトウェアのデザイン技術に専念しています。医療、教育、物流などの分野の創業会社に投資したことがあります。2013年からビットコインのブロックチェーンの進展に関心を持って、コミュニティーで宣伝しています。

2014年モントリオールIT協会を創設し、会員が700人以上、イベントが百回以上です。ブロックチェーンや人口知能、ビッグデータなどの先端技術に関する講座を数回主催しました。

2017年7月、カナダのケベックでExpress Computing Inc（ビットコインのマイニング会社）を創設しました。マイニングマシンのデザイン、マイニング、販売が同時に行なっています。

曹は長年来北米のブロックチェーンコミュニティーで活躍し、多くのICO商品を分析しています。

林欽輝　プロジェクトマネージャー

起業と銀行業界で13以上のコンサルティングと開発経験を持っています。300万ユーザーのSNS アプリのCTOを務めたことがあります。そのほかに、

Wellsfargo や GE Capital、Laurentian Bank などの銀行に 7 年以上のコンサルティングと開発をしたことがあります。NBAI では、林はブロックチェーンのプログラミング、仮想通貨のマイニング、人工知能との統合に従事し、効率的なブロックチェーン・人口知能エコシステムの構築に取り組んでいます。

熊騰科博士　AI Architect

カナダのシャーブルック大学でコンピュータ科学の博士で、10 年の人工知能開発経験を持っています。多くの人工知能会社で CTO を務めたことがあります。中国科学院深圳先端技術研究所の訪問学者です。データマイニング分野のトップレベルの会議と雑誌で 6 つの論文を発表しました。NBAI では、プロジェクトのアーキテクチャと企画を担当しています。

李岩岩　CFO

CFA で、カナダ CPA の準会員です。TQC 投資などの大手企業で働いたことがあります。中国の証券市場とカナダの投資市場で長年の経験を積み重ねました。中国とカナダの金融・会計分野の知識を熟知しています。財務管理、税務企画、融資分野の専門家です。

姚璐　人工知能エンジニア

HK Financial Invest. PLC と AXA (HK)でアナリストを務めたことがあります。コンコルディア大学の経済学修士です。長年の量的金融研究、リスク管理経験を持っています。Python and R 言語に精通しています。現在は主に金融分野においてディープラーニングと神経ネットワークアルゴリズムの応用を研究しています。

厙通　ブロックチェーン開発者

コンコルディア大学のコンピュータ修士です。Ethash や DPOS などのブロックチェーンアルゴリズムに精通しています。ブロックチェーン製品のアーキテクチャのデザインと実施を担当しています。

张恺谌　人工知能エンジニア

華南理工大学の学士、コンコルディア大学のコンピュータ科学修士です。Java や Python、Javascript などのプログラミングに精通しています。華南理工

大学の教材の作者です。長年のマーケティングと管理経験を持っています。現在は語義分析とディープラーニングの研究を中心にしています。

严如华　ベテランのフルスタックエンジニア

福州大学卒業、南米、ヨーロッパ、北米などの地域で 10 年以上のソフトウェアの開発経験を持っています。Python や Node.js などのプログラミング言語に精通しています。最適化、コード分析が得意です。

Alberto Lacerda フロントエンドエンジニア

Laureate International Universities で計算機科学を専攻にしていました。10 年の IT 分野の経験を持っています。Accenture の開発者を務めたことがあります。現在は NBAI でフロントエンドエンジニアを務めています。

張馳　バックエンドエンジニア

コンコルディア大学のコンピュータ修士です。Python や Js、Java の関係技術、フレームワークに熟知しています。現在は NBAI でプログラムのバックエンドサービスの開発とメンテナンスを担当しています。

周品　ソフトウェアエンジニア

ハルピン理工大学から卒業、計算機科学の修士学位を取得しました。IT 開発分野で 8 年以上の経験があります。現在は NBAI でソフトウェアエンジニアを務めています。

沈思迪　UI デザイナー

アメリカのリーハイ大学のグラフィックデザイン専攻の修士です。大手企業で長年のデザイン経験があります。NBAI の産品、宣伝資料のデザイン、マーケティングを担当しています。

Alecsa Tabisaura UI デザイナー

カナダのモントリオールの Cégep Marie-Victorin でグラフィックデザインを専攻していました。フリーデザイナーとして多くの会社に作品をデザインしたことがあります。現在は NBAI で UI デザイナーを務めています。

徐峥　Executive Assistant & Marketing Coordinator

中国伝媒大学のアナウンサー専攻から卒業。言語教育、旅行などの分野で働いたことがあります。長年の営業とマーケティング経験を持っています。現在は NBAI で事務とマーケティングを担当しています。

Jessica Boxerman マーケティング専門家

ヨーロッパや北米の多くのコミュニティーで活躍し、長年のマーケティング経験を持っています。欧米コミュニティーの運営、ブランド宣伝、広報、パブリック・リレーションズなどを担当しています。

徐琰　フロントエンドエンジニア

北京大学から卒業、モントリオール理工学院の修士です。SAP で Web 開発者を務めたことがあります。現在は Nebula AI の Web 開発チームのリーダーです。

张夢媛博士　エンジニア

カナダの Concordia 大学でデータセキュリティ人工知能博士学位を取得しましたネットセキュリティなどを研究しています。多くの会社でネットセキュリティと人工知能研究を行なっています。

梁敏　人工知能エンジニア

マギル大学の修士、モントリオールディープラーニング学院の修士です。機械学習を 3 年間研究しました。ハーバード大学やマギルコンピュータネット研究室で人工知能の関連研究を行なったことがあります。RNN、CNN、LSTM など多くの人工知能ニューラルネットワークアルゴリズムを研究して、いくつかの論文を発表しました。

王赞　人工知能エンジニア

コンコルディア大学の修士です。10 年以上のデータ分析経験があります。LG や SK などの大手企業で働いたことがあります。自然言語処理やデータの処理などを担当しています。長年来、RNN、CNN、LSTM など多くの人工知能ニューラルネットワークアルゴリズムを研究しています。

Carlos Gonzalez Oliver ブロックチェーンエンジニア

マギル大学のコンピュータ科学の博士です。機械学習の専門知識とプロジェクト経験を持っています。科学理論におけるブロックチェーンの応用に専念しています。

9.2 顧問チーム

Yan Liu コンコルディア大学クラウドコンピューティング及び分散型システムの教授

コンコルディア大学クラウドコンピューティング及び分散型システムの教授です。百篇以上の論文を発表しました。9 年以上の防御システムの開発経験があります。アメリカの Department of Energy Pacific Northwest National Laboratory (PNNL) や National ICT Australia (NICTA)で高級エンジニアを務めたことがあります。

林振华博士　人工知能顧問

カリフォルニア大学デービス校の博士課程修了者で、数理統計研究をしています。2011 年と 2013 年にカナダのサイモンフレーザー大学でコンピュータ科学の修士学位と統計学の修士学位を取得しました。2017 年トロント大学の統計博士卒業。統計機械学習や分散型機械学習などに興味を持っています。

史遜博士　ブロックチェーン顧問

アメリカシリコンバレーの Harmonic Inc で働いています。2012 年トロントのヨーク大学の博士学位を取得しました。2006 年北京航空航天大学から卒業。ブロックチェーンや暗号学などに自分の考え方を持っています。

Louis Cleroux　ブロックチェーン専門家

Louis は起業家と協力し、イーサリアムとビットコインなどのブロックチェーン技術を改善しようとしています。最近の投資対象はスマートウォレットやスマートアプリケーションなどに集中しています。

関宇　ブロックチェーン顧問

関は. NET / C# / Azure Cloud/DevOps/マイクロソフトの技術専門家です。20

年以上のソフトウェアデザイン・開発経験を持っています。マイクロソフトのアジア研究センターで働いたことがあります。マイクロソフトの CEO Satya Nadella が授与した「Microsoft Most Valuable Professional (MVP)」というアワードを獲得したことがあります。

朱斌　クラウドコンピューティング顧問

15 年のデータベース研究経験を持っています。ビッグデータの科学家です。Huawei や MindGeek などで働いたことがあります。RMDB、NoSQL db などに精通しています。長年来チームを管理して、チームメンバーとの交流やコーディネーションが得意です。

Adam Allouba　法律顧問

世界最大な法律事務所 Dentons のパートナーで、Dentons の全ての法律関係の仕事を担当して、投資家の利益を守り、会社が各国法律に違反しないことを保証しています。

Douglas Leahey　ビジネス発展顧問

環境学の博士で、モントリオール青年就職の顧問を務めています。法律や融資、政府のイノベーションサポートプロジェクトのアドバイザーサービスを提供します。会社の戦略とマーケティングプランに参与します。

Jake Barralet　産学連携プロジェクト Mitac 顧問

ロンドン大学の博士です。ボーングラフトと生物材料を研究しています。Nebula AI と協力し、生物医学において人工知能の応用を探求しています。

10　終わりに

世界初の人工知能ブロックチェーンシステムとして、Nebula AI が人工知能の技術革新を促し、ブロックチェーンに基づくトラストメカニズムを構築することに取り組んでいます。NBAI が次世代の人工知能ブロックチェーンの基礎プラットフォームを構築したので、開発者はシステムや環境を配慮せずに、効率的、コストの低い、安全安心な開発・計算・配置に専念することができるようになります。

NBAI は分散型データコンセンサスシステムです。NBAI トークンが価値のキャリヤーとして、NBAI システムにおいて人工知能の価値の流れを実現します。従来のネット技術はデータの通信問題を解決しましたが、NBAI はそれを踏まえて、データのコンセンサス問題を解決します。集中型プラットフォームに比べて、NBAI はデータをサービスプロバイダに保存することで、漏洩などを回避します。これでタスクを処理すると同時にデータの私有を実現しました。ブロックチェーン技術の発展によって、デジタル化信用社会が可能になりました。NBAI はこれからもブロックチェーン技術の発展に力を注ぎ、人工知能のより良い発展に取り組みます。

参考文献

Iris Belle. The architecture, engineering and construction industry and blockchain technology.

Juan Benet. Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561, 2014.

Evangelos Benos, Rod Garratt, and Pedro Gurrola-Perez. The economics of distributed ledger technology for securities settlement. 2017.

Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. white paper, 2014.

Matteo Campanelli, Rosario Gennaro, Steven Goldfeder, and Luca Nizzardo. Zero-knowledge contingent payments revisited: Attacks and payments for ser- vices. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pages 229–243. ACM, 2017.

Sinclair Davidson, Primavera De Filippi, and Jason Potts. Economics of blockchain. 2016.

Ben Laurie and Richard Clayton. Proof-of-work proves not to work; version 0.2. In Workshop on Economics and Information, Security, 2004.

June Ma, Joshua S Gans, and Rabee Tourky. Market structure in bitcoin mining. Technical report, National Bureau of Economic Research, 2018.

marketsandmarkets.com. Blockchain market worth 7,683.7 million usd by 2022. https://www.marketsandmarkets.com/PressReleases/ blockchain-technology.asp/.

J-P Martin and Lorenzo Alvisi. Fast byzantine consensus. IEEE Transactions on Dependable and Secure Computing, 3(3):202–215, 2006.

David C Mills, Kathy Wang, Brendan Malone, Anjana Ravi, Jeffrey C Mar- quardt, Anton I Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kargenian, et al. Distributed ledger technology in payments, clearing, and set- tlement. 2016.

Armin Nabaei, Melika Hamian, Mohammad Reza Parsaei, Reza Safdari, Taha Samad-Soltani, Houman Zarrabi, and A Ghassemi. Topologies and performance of intelligent algorithms: a comprehensive review. Artificial Intelligence Review, 49(1):79–103, 2018.

Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

Nvidia. Geforce gtx 1080 ti. https://www.nvidia.com/en-us/geforce/products/10series/geforce-gtx-1080-ti/#performance.

Svein Ølnes. Beyond bitcoin enabling smart government using blockchain technology. In International Conference on Electronic Government and the Infor- mation Systems Perspective, pages 253–264. Springer, 2016.

OntarioHydro. Electricity rates by province. http://www.ontario-hydro.com/electricity-rates-by-province.

Wessel Reijers, Fiachra O'Brolcháin, and Paul Haynes. Governance in blockchain technologies & social contract theories. Ledger, 1:134–151, 2016.

Klaus Schwab, Xavier Sala-i Martin, et al. The global competitiveness report 2010-2011. Citeseer, 2010.

Brett Scott. How can cryptocurrency and blockchain technology play a role in building social and solidarity finance? Technical report, UNRISD Working Paper, 2016.

Marten Van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In Annual International Confer- ence on the Theory and Applications of Cryptographic Techniques, pages 24–43. Springer, 2010.

MGCSA Walport. Distributed ledger technology: Beyond blockchain. UK Government Office for Science, 2016.

Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In Security and Privacy Workshops (SPW), 2015 IEEE, pages 180–184. IEEE, 2015.

A　修正歴史

2018.2.28 私募段階のハードキャップを 25,000 ETH から 18,000 ETH に修正しました。

公募段階のハードキャップを 24,000 ETH から 12,000 ETH に修正しました。

10MW の人工知能コンピューティングセンターの建設計画をキャンセルしました。

「大規模な第三者インターネットデータセンターと協力し、AI のコンピューティングに計算力を提供する」と修正しした。

協力パートナーとプロジェクトの修正。

トークンの分配割合の修正。

顧問チームに新しいメンバーを加えました。

2018.3.17 開発チームに新しいメンバーを加えました。

2018.3.16 私募の時間を修正しました。